REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed May 20, 2005. In order to advance prosecution of this case, Applicants amend Claims 1, 5, 10-12, 14, and 17. Applicants cancel Claims 6, 7, 18, and 19 without prejudice or disclaimer. Applicants respectfully request reconsideration and favorable action in this case.

Section 102 Rejections

The Examiner rejects Claims 1-7 and 10-19 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,398,196 issued to Chambers ("*Chambers*"). As amended Claim 1 recites:

> A method of detecting viral code in subject files, comprising:
> creating an artificial memory region spanning one or more components of the operation system;
> creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values;
> emulating execution of computer executable code in a subject file; and
> detecting when the emulated computer executable code attempts to access the artificial memory region.

Chambers fails to recite, expressly or inherently, every element of amended Claim 1. For example, *Chambers* fails to recite "creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values." The portion of Chambers cited by the Examiner in rejecting similar elements in original Claim 7, however, states only that:

> Block 550 is illustrated in further detail by FIG. 8. This control of operating system entry points need not be performed to obtain substantial benefits from the emulation of the target program; however, this process does a higher level of control over the target program and also allows for a more accurate evaluation of viral behavior on the part of the target program.
> From beginning block 800 control passes to block 810, at which the monitor program examines a list of operating system entry points to determine if any have changed as a result of the instruction just emulated. This would indicate that the target program had replaced an interrupt handler with a routine of its own.
> . . .
> After block 840, execution passes to block 850, which returns control to the basic process of FIG. 5. This causes the interrupt handler routine of FIG. 9 to be emulated in the same step by step manner as the target program. This maintains the highest degree of encapsulation around the target program,

> although if detecting viral replication is essentially the only concern, the interrupt handler testing routine of FIG. 9 may alternatively be executed in a more straightforward emulation without many of the execution safeguards described above.
>
> Col. 9, ll. 13-25 and 44-54.

The cited portion of *Chambers* however fails to disclose any "custom version of [an] export table [associated] with a plurality of entry points [wherein] the entry points comprise predetermined values[.]" In rejecting Claim 6, the Examiner asserts that "the export table of operating system components [recited by Claim 6] is represented by a 'list of operating system entry points.'" *Office Action*, p. 4. To whatever extent this may be true, *Chambers* does not indicate that the list of operating system entry points "comprise[s] predetermined values." Thus, *Chambers* fails to disclose any "export table [that] is associated with a plurality of entry points [wherein] the entry points comprise predetermined values."

Moreover, the cited portion of *Chambers* fails to disclose the creation of any export tables. The cited portion merely describes a process for monitoring the list of operating system entry points for changes. Consequently, even to the extent that the list of operating system entry points disclosed by *Chambers* can be equated with the export table of Claim 1, *Chambers* further fails to disclose "creating a custom version of an export table[.]" Thus, *Chambers* fails to disclose "creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values" as recited by amended Claim 1.

As a result, *Chambers* fails to disclose every element of amended Claim 1. Claim 1 is thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of amended Claim 1 and its dependents.

Although of differing scope from Claim 1, Claims 10-12 and 14 include elements that, for reasons substantially similar to those discussed with respect to Claim 1, are not disclosed by the cited reference. Claims 10-12 and 14 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 10-12 and 14, and their respective dependents.

Additionally, many of the dependents of Claim 1 include other elements that are also not disclosed in the cited reference. For example, Claim 5 as amended recites:

> The method of claim 1, further comprising:

monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping; and

determining based on a detection of looping whether the emulated computer executable code is viral.

Chambers fails to recite, expressly or inherently, additional elements of amended Claim 5. *Chambers* fails to disclose "monitoring accesses by the emulating computer executable code to the artificial memory region to detect looping." The portion of *Chambers* cited by the Examiner in rejecting this claim discloses use of a guinea pig file to determine whether certain viral code displays replicative behavior. Col. 10, ll. 40-43. While the cited portion of *Chambers* references "recursion," it describes recursively executing the emulation process and merely discusses terminating emulation if viral behavior by the target program is confirmed while recursively executing the emulation. *Chambers* does not disclose "monitoring accesses by the emulating computer executable code to the artificial memory region to detect looping" as recursion is assumed to be part of this process.

Chambers also fails to disclose "determining based on a detection of looping whether the emulated computer executable code is viral." The cited portion of *Chambers* describes a process for determining whether a virus has corrupted the interrupt handlers of a computer system. More specifically, the system in *Chambers* emulates execution of a target program, and then accesses a first "guinea pig file" to determine if execution of the target program has corrupted the interrupt handlers. Col. 9, ll. 44-48; col. 9, ll. 61-64; col. 10, ll. 7-10. Following access of the first guinea pig file, the system determines whether any unauthorized modification of the first guinea pig file has occurred, i.e. whether block 960 of FIG. 9 has been reached. Col. 10, ll. 10-23. If so, the described system of *Chambers* may further test the replicative nature of the virus initiated by the target program, by executing the first guinea pig file and then accessing a second guinea pig file. Col. 10, ll. 32-40. Following access of the second guinea pig file, the system determines whether any unauthorized modification of the second guinea pig file has occurred, i.e. whether block 960 has been reached again. In other words, "if block 960 is reached during the second level of emulation, viral behavior is confirmed and the second level of emulation is terminated." Col. 10, ll. 43-50. Thus, the system of *Chambers* determines whether viral behavior has occurred based on whether a first file exposed to unauthorized modification will cause unauthorized modification of other files if the first file is later executed. *Chambers* does not however disclose "determining based on

a detection of looping whether the emulated computer executable code is viral" as recited by amended Claim 5.

As a result, *Chambers* fails to recite, expressly or inherently, at least these additional elements of Claim 5. Thus, for at least these additional reasons, Claim 5 is allowable. As noted above, Applicants respectfully request reconsideration and allowance of amended Claim 5, as noted above.

Although of differing scope from Claim 5, amended Claim 17 includes elements that, for reasons substantially similar to those discussed with respect to Claim 5, are not disclosed by the cited reference. Claim 17 is thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of amended Claim 17, as noted above.

Additionally, Applicants cancel Claim 6, 7, 18, and 19 without prejudice or disclaimer. Applicants wish to note that, with respect to all cancellations and amendments herein, Applicants reserve the right to pursue broader subject matter than that currently claimed through the filing of continuations and/or other related applications.

Section 103 Rejections

The Examiner rejects Claims 8, 9, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Chambers in view of U.S. Patent No. 5,974,549 issued to Golan ("*Golan*"). Claims 8 and 9 depend from Claim 1, which has been shown above to be allowable. Claim 20 depends from Claim 14, which has been shown above to be allowable. Claims 8, 9, and 20 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 8, 9, and 20, as noted above.

Conclusions

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicants stands ready to conduct such a conference at the convenience of the Examiner.

No fees are believed to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Todd A. Cason
Reg. No. 54,020

2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6452

Date: 8/22/05

CORRESPONDENCE ADDRESS:

Customer Number: **05073**